Linear Algebra and its Applications 436 (2012) 3160–3164

Contents lists available at SciVerse ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

Roots multiplicity and square-free factorization of polynomials using companion matrices

N.H. Guersenzvaig [a], Fernando Szechtman [b,*]

[a] *Av. Corrientes 3985 6A, (1194) Buenos Aires, Argentina*
[b] *Department of Mathematics and Statistics, University of Regina, Saskatchewan, Canada*

ARTICLE INFO

Article history:
Received 21 September 2011
Accepted 19 October 2011
Available online 30 November 2011

Submitted by V. Sergeichuk

AMS classification:
12D05
13A05
15A24

Keywords:
Lagrange Interpolation Formula
Square-free factorization
Companion matrix

ABSTRACT

Given an arbitrary monic polynomial f over a field F of characteristic 0, we use companion matrices to construct a polynomial $M_f \in F[X]$ such that for each root α of f in the algebraic closure of F, $M_F(\alpha)$ is equal to the multiplicity $m(\alpha)$ of α as a root of f. As an application of M_f, we give a new method to compute each component of the square-free factorization $f = P_1 P_2^2 \cdots P_m^m$, where $P_k \in F[X]$ is the product of all $X - \alpha$ with $m(\alpha) = k$ for $k = 1, \ldots, m = \max m(\alpha)$.

1. Introduction

We fix throughout the paper a field F of characteristic 0 and a monic polynomial $f \in F[X]$ of degree n. We say that f is square-free if for any monic polynomial $g \in F[X]$: $g^2|f$ implies $g = 1$, or, equivalently, if $\gcd(f, f') = 1$. We assume henceforth that $n \geqslant 1$ and that f has prime factorization

$$f = f_1^{m_1} \cdots f_r^{m_r}, \tag{1.1}$$

so f is square-free if and only if each $m_j = 1$. Set $m = \max_{1 \leq j \leq r} m_j$ and collect in P_k all monic irreducible factors f_j of f having multiplicity $m_j = k$ in (1.1), that is,

* Corresponding author.
E-mail addresses: nguersenz@fibertel.com.ar (N.H. Guersenzvaig), fernando.szechtman@gmail.com (F. Szechtman).

doi:10.1016/j.laa.2011.10.018

$$P_k = \prod_{\substack{1 \le j \le r \\ m_j = k}} f_j, \quad k = 1, \ldots, m.$$

Each P_k is square-free, yielding the so-called square-free factorization of f, namely

$$f = P_1 P_2^2 \cdots P_m^m. \tag{1.2}$$

Efficient algorithms to compute (1.2) were developed about forty years ago by Tobey [7], Horowitz [4,5], Musser [6] and Yun [8]. A more recent algorithm can be found in [1]. The square-free factorization (1.2) is usually utilized as a first step towards the computation of the full factorization (1.1) as well as to integrate rational functions, following a method due to Hermite [3], as explained in [1].

Let us review the Tobey–Horowitz algorithm, one of the simplest known methods to obtain (1.2). Let $g = f_j$, where $1 \leqslant j \leqslant r$, and set $k = m_j$ as well as $h = f/g^k$. We then have $f = g^k h$ with $\gcd(g, h) = 1$. Moreover,

$$f' = kg^{k-1}g'h + g^k h'.$$

As g is relatively prime to $kg'h$, the multiplicity of g in $\gcd(f, f')$ is $k-1$. Hence

$$\gcd(f, f') = P_2 P_3^2 \cdots P_m^{m-1}.$$

Setting

$$D_0 = f, \quad D_1 = \gcd(D_0, D_0'), \quad D_2 = \gcd(D_1, D_1'), \ldots$$

a repeated application of the preceding discussion yields

$$D_k = \begin{cases} P_{k+1} P_{k+2}^2 \cdots P_m^{m-k} & k = 0, \ldots, m-1, \\ 1 & k \geqslant m, \end{cases}$$

whence

$$\frac{D_{k-1}}{D_k} = P_k P_{k+1} \cdots P_m, \quad k = 1, \ldots, m-1. \tag{1.3}$$

Therefore, not only m can be recognized as the smallest positive integer k such that $D_k = 1$, but we also have

$$P_k = \frac{D_{k-1}}{D_k} : \frac{D_k}{D_{k+1}} = \frac{D_{k-1}D_{k+1}}{D_k^2}, \quad k = 1, \ldots, m.$$

In this paper we furnish an entirely new practical method to compute (1.2) by means of Lagrange Interpolation Formula and companion matrices.

Let K be an splitting field of f over F and let $S(f)$ be the set of roots of f in K, whose size will be denoted by s. For each $\alpha \in S(f)$ let $m(\alpha)$ be the multiplicity of α as a root of f. Lagrange Interpolation Formula ensures the existence and uniqueness of a polynomial $M_f \in K[X]$ of degree less than s satisfying

$$M_f(\alpha) = m(\alpha), \quad \alpha \in S(f). \tag{1.4}$$

The polynomial $f_0 = f_1 \cdots f_r$ is called the square-free part of f. Clearly,

$$f_0 = \prod_{1 \leqslant j \leqslant s} (X - \alpha_j) = P_1 \cdots P_m.$$

Applying case $k = 1$ of (1.3) we obtain

$$f_0 = f / \gcd(f, f').$$

Combining the two preceding equations we obtain

$$P_k = \prod_{\substack{1\le j\le s\\ m(\alpha_j)=k}} (X-\alpha_j) = \gcd(M_f - k,\ f/\gcd(f,f')), \quad k=1,\dots,m. \tag{1.5}$$

The practical use of (1.5) seems to be limited due to the mysterious nature of M_f. A closer look reveals that

$$M_f = \sum_{\alpha\in S(f)} \frac{m(\alpha)}{f_0'(\alpha)} \frac{f_0}{X-\alpha}, \tag{1.6}$$

which can be verified by evaluating both sides at each $\alpha \in S(f)$. This seems to confirm the ineffectiveness of (1.5), as (1.6) requires the use of all roots of f in K. However, applying the Galois group $G = \mathrm{Gal}(K/F)$ to (1.4) we see that $M_f \in F[X]$. Indeed, let $\sigma \in G$. Then

$$M_f^{\sigma}(\alpha^{\sigma}) = M_f(\alpha)^{\sigma} = m(\alpha)^{\sigma} = m(\alpha) = m(\alpha^{\sigma}) = M_f(\alpha^{\sigma}),$$

so $M_f^{\sigma} = M_f$ by uniqueness, whence $M_f \in F[X]$, as claimed. The fact that $M_f \in F[X]$ suggests that there should be a rational procedure to obtain M_f from f. This is exactly what we do in this paper, by means of companion matrices.

The outcome is an efficient procedure to compute all components P_k of (1.2). Indeed, first compute $f_0 = f/\gcd(f,f')$, then M_f, as indicated in §2, and then proceed sequentially to find all $P_1, P_2, \dots$ making use of (1.5), stopping at m, namely the smallest positive integer k satisfying $\deg(P_1) + 2\deg(P_2) + \cdots + k\deg(P_k) = n$.

2. Using companion matrices to find M_f from f

Given a monic polynomial $g = g_0 + g_1X + \cdots + g_{s-1}X^{s-1} + X^s \in F[X]$ of positive degree s, its companion matrix $C_g \in M_s(F)$ is defined

$$C_g = \begin{pmatrix} 0 & 0 & \cdots & 0 & -g_0 \\ 1 & 0 & \cdots & 0 & -g_1 \\ 0 & 1 & \cdots & 0 & -g_2 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -g_{s-1} \end{pmatrix}.$$

We will use below the well-known fact that $g(C_g) = 0$. Let $F_s[X]$ be the subspace of $F[X]$ with basis $1, X, \dots, X^{s-1}$ and let $[R] \in F^s$ stand for the coordinates of $R \in F_s[X]$ relative to this basis. We will also use the following formula from [2]:

$$R(C_g) = ([R]\ \ C_g[R]\ \ C_g^2[R]\ \cdots\ C_g^{s-1}[R]). \tag{2.1}$$

Since the first column of a product of matrices, say AB, is equal to the product of A by the first column of B, it follows from (2.1) that for any $P, Q, T \in F_s[X]$,

$$P(C_g)Q(C_g) = T(C_g) \iff P(C_g)[Q] = [T]. \tag{2.2}$$

Theorem 2.1. *Let F be a field of characteristic 0 and let $f \in F[X]$ be monic of degree $n \geqslant 1$. Set $f_0 = f/\gcd(f,f')$, $s = \deg(f_0)$ and $P = f'/\gcd(f,f')$. Let M_f, $S(f)$ and $m(\alpha)$ be as in the Introduction. Then there exist unique $g \in F_s[X]$ and $h \in F[X]$ such that $f_0'g + f_0h = 1$. Moreover, for such P, f_0 and g,*

$$[M_f] = P(C_{f_0})[g].$$

Proof. Since f_0 is the square-free part of f, it is clear that $\gcd(f_0, f_0') = 1$. This ensures the existence and uniqueness of g and h. Let R be the remainder of dividing $M_f f_0'$ by f_0. By Lagrange Interpolation

Formula, we have

$$R = \sum_{\alpha \in S(f)} \frac{R(\alpha)}{f_0'(\alpha)} \frac{f_0}{X-\alpha} = f_0 \sum_{\alpha \in S(f)} \frac{m(\alpha)}{X-\alpha} = f_0 \frac{f'}{f} = P.$$

Therefore,

$$M_f(C_{f_0}) f_0'(C_{f_0}) = R(C_{f_0}) = P(C_{f_0}).$$

But $f_0'(C_{f_0})g(C_{f_0}) = I_s$, so

$$M_f(C_{f_0}) = P(C_{f_0})g(C_{f_0}),$$

which by (2.2) is equivalent to what we want to prove. □

Example 2.2. Let $f = X^4 - 4X + 3 \in \mathbb{Q}[X]$. Then

$$f' = 4X^3 - 4 \text{ and } \gcd(f, f') = X - 1,$$

so

$$f_0 = X^3 + X^2 + X - 3, \quad f_0' = 3X^2 + 2X + 1 \quad \text{and} \quad P = 4X^2 + 4X + 4.$$

We achieve $f_0'g + f_0h = 1$ by taking

$$g = (1/72)X^2 + (1/9)X + (1/24), \quad h = (-1/24)X - (23/72).$$

Using

$$C_{f_0} = \begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}, \tag{2.3}$$

we obtain

$$[M_f] = ([P] \;\; C_{f_0}[P] \;\; C_{f_0}^2[P])[g] = \begin{pmatrix} 4 & 12 & 0 \\ 4 & 0 & 12 \\ 4 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1/24 \\ 1/9 \\ 1/72 \end{pmatrix} = \begin{pmatrix} 3/2 \\ 1/3 \\ 1/6 \end{pmatrix},$$

which means

$$M_f = \frac{1}{6}X^2 + \frac{1}{3}X + \frac{3}{2}. \tag{2.4}$$

Next we compute

$$P_1 = \gcd(M_f - 1, f_0) = X^2 + 2X + 3, \quad P_2 = \gcd(M_f - 2, f_0) = X - 1,$$

which yields the square-free factorization, $f = P_1P_2^2$.

Remark 2.3. It is possible to find the degrees of the P_k's before actually computing these polynomials. This can be done as follows. Suppose f_0 has roots $\alpha_1, \dots, \alpha_s$ in K. Then C_{f_0} is similar to the diagonal matrix $\mathrm{Diag}(\alpha_1, \dots, \alpha_s)$, so $M_f(C_{f_0})$ is similar to $\mathrm{Diag}(m(\alpha_1), \dots, m(\alpha_s))$ and has characteristic polynomial

$$\mathrm{Char}\, M_f(C_{f_0}) = \prod_{1 \le i \le s} (X - m(\alpha_i)) = \prod_{1 \le k \le \max m(\alpha_i)} (X - k)^{\deg(P_k)}.$$

For instance, in Example 2.2 we can use (2.3) and (2.4) to obtain

$$M_f(C_{f_0}) = \begin{pmatrix} 3/2 & 1/2 & 1/2 \\ 1/3 & 4/3 & 1/3 \\ 1/6 & 1/6 & 7/6 \end{pmatrix}.$$

Therefore

$$\mathrm{Char}_{M_f(C_{f_0})} = X^3 - 4X^2 + 5X - 2 = (X-1)^2(X-2),$$

which indicates the square-free factorization $f = P_1P_2^2$, with $\deg(P_1) = 2$ and $\deg(P_2) = 1$, in complete agreement with what we found above.

Remark 2.4. Let R be an integrally closed domain of characteristic 0 with field of fractions F, and let $f \in R[X]$ be monic of degree $n \geqslant 1$. Then the square-free components of f, as found above, will have coefficients in R. Indeed, (1.2) shows that all α_i, and hence the coefficients of all P_k, are integral over R. But these coefficients are in F, and hence lie in R.

Acknowledgement

We thank V. Sergeichuk for valuable comments.

References

[1] J. Gerhard, Fast modular algorithms for squarefree factorization and Hermite integration, Appl. Algebra Eng. Comm. Comput. 11 (2001) 203–226.
[2] N.H. Guersenzvaig, F. Szechtman, A closed formula for the product in simple integral extensions, Linear Algebra Appl. 430 (2009) 2464–2466.
[3] C. Hermite, Sur l'integration des functions rationelles, Ann. of Math. (2) 11 (1872) 145–148.
[4] E. Horowitz, Algorithms for symbolic integration of rational functions, Ph.D. Thesis, University of Wisconsin, 1969.
[5] E. Horowitz, Algorithms for partial fraction decomposition and rational function integration, Proc. ACM Symp. Symbolic Algebraic Manipulation (1971) 441–457.
[6] D.R. Musser, Algorithms for polynomial factorization, Ph.D. Thesis, University of Wisconsin, 1971.
[7] R.G. Tobey, Algorithms for antidifferentiation of rational functions, Ph.D. Thesis, Harvard, 1967.
[8] D.Y.Y. Yun, On square-free decomposition algorithms, Symbolic and algebraic computation, in: Proc. 1976 ACM Symp, 1976, pp. 26–35.